Lab 1: Man-in-the-middle attack (ARP spoofing)

Pomoćne komande

- `pwd` - file path foldera u kojem se trenutno nalazimo
- `cd` - promjeni direktorij
- `ls` - izlistaj fileove unutar direktorija
- `mkdir` - kreiraj direktorij
- `wsl` - Windows Subsystem for Linux

Zadatak:

Izvršavanje man in the middle napada (MitM) u virtualnoj Docker mreži i denial od service (DoS) napada iskorištavanjem ranjivosti ARP protokola.

Žrtve napada:

1. `station-1`
2. `station-2`

Napadač:

1. `evil-station`

Koraci:

1. kloniranje repozitorija

- git clone https://github.com/mcagalj/SRP-2022-23

2. mijenjanje radnog direktorij

- cd SRP-2022-23/arp-spoofing/

3. buildanje i pokretanje docker kontejnera

- ./start.sh

4. zaustavljanje docker kontejnera

- ./stop.sh

5. pokretanje interaktivnog shella u station-1 kontejneru

- docker exec -it station-1 bash

6. provjeravanje nalazi li se station-2 na istoj mreži

- ping station-2

7. pokretanje interaktivnog shella u station-2 kontejneru

- docker exec -it station-2 bash

8. uspostavljanje komunikacije između station-1 i station-2

- netcat -l -p 8080

- netcat station-2 8080

9. pokretanje interaktivnog shella u evil-station kontejneru

- docker exec -it evil-station bash

10. evil-station predstavlja se stationu-1 kao station-2 (osluškivanje promet na mrežnoj kartici) - narušavanje **integriteta** i **povjerljivosti**

- arpspoof -t station-1 station-2

- tcpdump

11. prekidanje prometa između station-1 i station-2 - narušavanje **dostupnosti**

- echo 0 > /proc/sys/net/ipv4/ip_forward